REMARKS/ARGUMENTS

Claims 1-83 were pending in the Office Action, and Applicants wish to thank the Examiner for the indication that the present application contains allowable subject matter. Specifically, claims 17, 18, 20-21, 23-24, 26-27, 29-30, 32-33, 74, 77, 80 and 83[1] were indicated to be allowable if written in independent format, and claims 3-5, 8-10, 13-15 and 82 were further indicated to be allowable if the rejections under 35 U.S.C. 112, second paragraph were overcome. Upon entry of the present amendment, claims 11-15, 35-71 and 73-75 are canceled without prejudice or disclaimer, claims 1, 6-10, 16, 19-27, 72, 77 and 82 are amended, and new claims 84-94 are added.

In the Office Action, claims 1-15 and 82 stand rejected under 35 U.S.C. 112, second paragraph as being indefinite; claim 76 is objected to as being a substantial duplicate of claim 75; and claims 1-2, 6-7, 11-12, 16-17, 19, 22, 25, 34, 72-73 and 75-78 stand rejected under 35 U.S.C. 102(e) as being anticipated by DeMello et al. (U.S. Patent No. 6,891,953). The rejections under 35 U.S.C. 112 and 37 C.F.R. 1.75 are rendered moot by the amendments contained herein, and the remaining rejections are addressed below.

Independent Claim 72 and Dependent Claims 76-78 and 82-83

The Office Action indicated that dependent claim 74 would be allowable if written in independent form, and Applicants have amended base independent claim 72 to recite language

[1] Claims 17 and 77 also appear among the listed claims in the Office Action's rejections, but since there is no substantive discussion in those paragraphs addressing these claims, Applicants assume these claims were not intended to be listed as rejected. However, Applicants respectfully request clarification as to the status of these claims if this is not the case.

found in claim 74 and intervening claim 73. Accordingly, independent claim 74, and remaining dependent claims 76-78 and 82-83 are believed to be allowable.

Independent Claim 1 and Dependent Claims 2-10 and 84-92

Amended independent claim 1 recites, among other features, the following steps:

> receiving a request to access encrypted content on a terminal;
>
> obtaining a license comprising a content decryption key and a set of binding attributes, the attributes including a public key of an authorized user of the encrypted content;
>
> in response to the request, polling a personal trusted device of said user to digitally sign data with a private key associated with the device;
>
> receiving said digitally signed data from said device

In rejecting claim 1, the Office Action cites DeMello et al. DeMello et al. relates to a method and system for binding software features to a persona, and the particular portion cited in the Office Action relates to selling an electronic book, or "eBook." The DeMello et al. system separates the sellers of eBooks (referred to as "retailers") from the entity that actually provides the eBooks to customers (referred to as a "fulfillment center"). See, e.g., col. 15, lines 1-47. The retailer and fulfillment center agree, in advance, on a secret symmetric key 75 to be used for encrypting and decrypting the eBook. Col. 15, lines 15-16. When the customer accesses the retailer's Internet site and purchases an eBook, the customer is shown a "receipt page" containing a URL link to the fulfillment center that will provide the eBook. Col. 15, lines 19-26. The link includes an encrypted parameter for the sale, and when the user clicks on that link, the encrypted parameter is sent to the fulfillment center, where it is decrypted using the secret symmetric key 75 to confirm to the fulfillment center that this user has purchased a copy of the eBook. See, e.g. col. 15, lines 26-29.

In the cited DeMello et al. purchase, the customer accesses the retailer's Internet site from the same computer that will receive the eBook, and there is no communication with another user device as part of the purchase. So, there is no teaching or suggestion in DeMello et al. of "in response to the request, polling a personal trusted device of said user to digitally sign data with a private key associated with the device," as recited in amended claim 1. Indeed, the secret key used in the DeMello et al. system is not known to any device of the user's. Instead, the secret key is known only to the fulfillment center and the retailer.

For at least these reasons, Applicants submit that amended independent claim 1 distinguishes over DeMello et al. Claims 2-10 and 84-92 depend from claim 1, and are allowable for at least the same reasons as claim 1, and further in view of the various features recited therein. For example, in addition to the claims that the Office Action has already indicated would be allowable, claim 84 recites that the personal trusted device is a mobile telephone. The DeMello et al. system does not use any mobile telephone as recited in claim 84. As another example, claim 90 recites a step of step of randomly generating textual data to be signed by the device. DeMello et al. uses no such randomly generated textual data.

Independent Claim 16 and Dependent Claims 17-27 and 93-94

Amended independent claim 16 recites, among other features, the following:

> a network interface which, in response to said terminal receiving a request to access said stored encrypted content, establishes a communication link between the terminal and at least one other terminal to request the other terminal to encrypt and digitally sign identity verification data using a private key stored at the other terminal, and which delivers the digitally signed identity verification data received from the other terminal to the protected processing environment; and

> wherein the protected processing environment uses said public key to decrypt said encrypted identity verification data, compares said decrypted data with said digital signature to verify the digitally signed data, and upon successful verification of the digitally signed data, the protected processing environment decrypts the encrypted content using the content decryption key.

In rejecting this claim, the Office Action does not identify the DeMello et al. elements that are alleged to correspond with the "terminal" and "other terminal" recited in the claim. As noted above, the DeMello et al. system essentially has three components: the retailer, the fulfillment center, and the user's computer. As described at col. 15 of DeMello et al., the DeMello et al. user makes a purchase by accessing the retailer's Internet site, and the site provides a receipt page containing a hyperlink to the fulfillment center, where the hyperlink also includes an encrypted parameter. See, e.g., col. 15, lines 15-25. Clicking on the link accesses the fulfillment center, provides it with the encrypted parameter, and the fulfillment center decrypts the parameter to determine whether the user has legitimately purchased a copy of the eBook. See, e.g., col. 15, lines 26-34.

The DeMello et al. encrypted parameter is encrypted using a secret key 75, and there is no teaching or suggestion that "the protected processing environment uses said public key to decrypt said encrypted identity verification data," as recited in amended claim 16. Furthermore, the DeMello et al. secret key is only shared between the retailer and fulfillment center, and there is no teaching or suggestion that either of these places includes "a storage for the encrypted content and a license, the license containing a content decryption key and a set of binding attributes, the attributes including a public key for a licensee of said content," as also recited in amended claim 16.

For at least these reasons, Applicants submit that amended claim 16 distinguishes over DeMello et al. Claims 17-27 and 93-94 depend from claim 16, and are allowable for at least the same reasons as claim 16, and further in view of the various features recited therein (indeed, many of these claims were already indicated as being allowable if written in independent form). For example, claim 93 recites "said identity verification data is a text string randomly generated by said other terminal." DeMello et al. does not teach or suggest the use of such data. Claim 94 recites that the "other terminal is a mobile telephone of said licensee," and DeMello et al. does not teach or suggest such a use of a mobile telephone.

CONCLUSION

All rejections having been addressed, Applicants respectfully submit that the instant application is in condition for allowance, and respectfully solicit prompt notification of the same. Should the Examiner believe that further discussion and/or amendment would be helpful, the Examiner is invited to telephone Applicants' undersigned representative at the number appearing below.

Respectfully submitted,
BANNER & WITCOFF, LTD.

Date: 4/12/2006

By: _____
Steve S. Chang
Registration No. 42,402

1001 G Street, N.W.
Eleventh Floor
Washington, D.C. 20001-4597
(202) 824-3000